Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-19. (Cancelled)

20. (Currently Amended) A method for protecting the processing of sensitive information in a security module having a monolithic structure, comprising at least an information ~~processing means~~processing device, ~~storage means~~storage device~~, distinct from said processing means,~~ for storing information capable of being processed by said ~~processing means~~processing device, means for checking the integrity of information and at least a data bus, wherein the transmitting of information through said data bus is secured ~~and in that it comprises~~by at least the following steps:

selecting a piece of sensitive information stored in the ~~storage means~~storage device;

determining a specific condition for the integrity of a datum of said selected information to be transmitted on said data bus;

reading, by the ~~processing means~~processing device, of said datum~~information~~ transmitted from the ~~storage means~~storage device to the ~~processing means~~processing device ~~for processing via a~~on said data bus;

processing said datum~~information~~ and executing a logic verification operation on all bits of said datum which is transmitted on said data bus~~verifying~~, by the ~~processing means~~processing device or by the means for checking the integrity of information, during the processing for verifying that the specific condition is satisfied; and

disabling the processing device~~of said information~~ if the specific condition is not satisfied.

21. (Currently Amended) The method according to claim 20, wherein said information datum is an operation code datum read in the ~~storage means~~storage device, all of the types of said operation code datum being contained in a table having a content determined during the manufacture of the security module, and the specific condition for the integrity of the information being said operation code datum~~the value of said information~~ is equal to a valid operation code datum~~one of several set values~~ of the table and at least operation code data composed by bits all equal to a same binary value are non valid operation code data of the table.

22. (Cancelled)

23. (Currently Amended) The method according to claim 20, wherein ~~the specific step of determining the condition for~~said means for checking the integrity of said information comprises a logic comparator and a first and second logic operator disposed each at different terminations of the data bus,~~calculating a first piece of integrity data, by means for checking the integrity of information, using the information read in the storage means,~~ said logic operators producing at least respectively a first and a second result compared tpgether by said logic comparator for verifying said specific condition for the integrity when there is an equality between said first and second results~~ comparing the first piece of integrity data to a second calculated piece of integrity data by means for checking the integrity of information, using the information received by said processing means and checking for equality, by said means for checking the integrity of information, between the first and second pieces of integrity data~~.

24. (Currently Amended) The method according to claim 23, wherein said logic selection input of both comparators is set to a~~a piece of integrity data is calculated from at least one piece of~~ calculation data whose value varies as a function of time.

25. (Currently Amended) The method according to claim 23, wherein said logic selection input of both comparators is set to a~~a piece of integrity data is calculated from at least one piece of~~ calculation data whose value varies randomly.

26. (Currently Amended) The method according to claim 20, wherein the disabling of the processing device~~of said information is~~ performed by ~~processing means~~ executing a microprogrammed instruction.

27. (Currently Amended) The method according to claim 26, wherein said~~the~~ microprogrammed instruction induces the following steps:

writing a piece of disable data into a nonvolatile location of the ~~storage means~~storage device; and

disabling the processing ~~of the information~~device.

28. (Currently Amended) The method according to claim 27 further comprising reading by the ~~processing means~~processing device said nonvolatile location of the ~~storage means~~storage device upon power up of said module before~~and~~ disabling the processing device~~module~~ if a value read at this location does not match.

29. (Currently Amended) A security module comprising an electronic circuit having a monolithic structure and comprising an information ~~processing means~~processing device, information ~~storage means~~storage device communicating with~~distinct from~~ said ~~processing means~~processing device via a data bus, and means for checking the integrity of information, the ~~processing means~~processing device selecting information data extracted from the ~~storage means~~storage device in order to process them~~it~~, wherein a specific condition for integrity concerning datum transmitted on the data bus is verified, by the ~~processing means~~processing device or by the means for checking the integrity of information,~~further comprising means for verifying a specific integrity condition of a piece of sensitive information~~, by executing a logic operation on all bits of said datum which is transmitted on said bus and further comprising means for disabling the processing device~~of the information, said means for disabling being activated~~ when said specific condition for integrity is not satisfied~~the means for verification or means for checking the integrity of information have detected that the specific condition is not satisfied~~.

30. (Currently Amended) A security module according to claim 29, wherein the ~~processing means~~processing device execute instructions data corresponding to operation codes extracted from a table defined during the building of the module, wherein the table comprises at least a forbidden instruction~~ value~~, ~~the forbidden values being defined during the building of the module~~and wherein said specific condition for integrity is not satisfied when said processing device process a forbidden instruction.

31. (Currently Amended) A security module according to claim 30, wherein at least an instruction data whose all bits are equal to a same binary value are forbidden instructions of said table~~the operation code to be processed is coded in the form of data bits, the security module comprising means for reading the values of all the bits and a disabling means activated when the values of the bits are all identical~~.

32. (Cancelled)

33. (Currently Amended) A security module according to claim ~~32~~29, wherein ~~the~~said means for disabling the processing device~~means~~ comprise means for irreversibly writing at least one indicator with an initial valid state in a non reversible modified invalid state, and means for reading said indicator during the next power-up of the module.

34. (Currently Amended) A security module according to claim 29, wherein said means for checking the integrity of information comprise at least two~~one~~ parity generator each disposed at terminations of the data bus~~cooperating with the storage means, at least one parity generator cooperating with the processing means,~~ and at least one comparator whose inputs are connected to and output of said~~each of the~~ parity generators, for verifying said specific condition for integrity when parity generators produce identical outputs by setting an output of said comparator linked to ~~and capable of inducing~~ an interrupt ~~in~~input of said the ~~processing means~~processing device.

35. (Currently Amended) A security module according to claim 34, wherein said output of both~~the operation of said~~ parity generator ~~varies as~~is set opposite according to a function of time.

36. (Currently Amended) A security module according to claim 34, wherein said output of both~~the operation of said~~ parity generators is set opposite ~~varies~~ randomly.

37. (Previously Presented) A security module according to claim 33, wherein the irreversible writing of said indicator is performed by executing a microprogrammed instruction.

38. (Previously Presented) A security module according to claim 29, wherein the security module is a microcircuit card.

39. (New) The method according to claim 23, wherein both logic operators are parity generators each having two logic opposite outputs and one logic selection input determines the one of said both logic outputs which is inputted in the comparator.